CLAIMS:

1. A network apparatus (2) comprising
- a biometry module (3) for detecting biometrical data of a user (1);
- a configuration module (4) which is adapted to determine an unambiguous network identifier and/or an unambiguous initial key from biometrical data provided by the biometry module (3) for the encrypted communication (particularly in the configuration phase) with a second apparatus.

2. An apparatus as claimed in claim 1, characterized in that it is adapted to eliminate the biometrical data of a user (1) after their use by the configuration module (4).

3. An apparatus as claimed in claim 1 or 2, characterized in that the communication with the second apparatus takes place in a wireless or wired way, particularly via a power supply mains.

4. An apparatus as claimed in any one of claims 1 to 3, characterized in that the configuration module is adapted to manage a list of biometrical data and/or data derived from said list for different users (1) of an authorized user group.

5. A method of assigning a network apparatus (2) to a network (A), wherein biometrical data of a user (1) are detected by the apparatus (2) and an unambiguous network identifier is derived therefrom, which identifier is used and known in the network (A) from previous and/or simultaneous inputs of the same biometrical data.

6. A method of configuring a communication connection between a network apparatus (2) and a network (A), wherein biometrical data of a user (1) are detected by the apparatus and an unambiguous initial key is derived therefrom, which initial key is known in the network (A) from previous and/or simultaneous inputs of the same biometrical data and is used for a secure communication (particularly in the configuration phase).